Cyber-security Considerations for Real-Time Physiological Status Monitoring: Threats, Goals, and Use Cases

John Holliman, Michael Zhivich, Roger Khazan, Albert Swiston, Brian Telfer
MIT Lincoln Laboratory, Lexington, MA
Email: {john.holliman,mzhivich,rkh,albert.swiston,telfer}@ll.mit.edu

***Abstract*—Real-time monitoring of physiological data can reduce the likelihood of injury in noncombat military personnel and first-responders. MIT Lincoln Laboratory is developing a tactical Real-Time Physiological Status Monitoring (RT-PSM) system named OBAN (Open Body Area Network), the purpose of which is to provide an open, government-owned framework for integrating multiple wearable sensors and applications. The current OBAN implementation accepts data from various sensors enabling calculation of physiological strain information, which may be used by squad leaders or medics to assess the team's health and enhance safety and effectiveness of mission execution. Security in terms of measurement integrity, confidentiality, and authentication is an area of interest because OBAN system components exchange possibly sensitive data in military applications. In this paper, we analyse potential cyber-security threats and their associated risks to an implementation of the OBAN architecture and identify directions for future research. The threat analysis is intended to inform the development of secure RT-PSM architectures.**

I. Introduction

The development of very low-power computing devices and wireless transceivers has improved the landscape of physiological-status monitoring and body area networks (BANs). A BAN is a wireless network composed of wearable computing devices, typically seen in medical and personal fitness settings. Real-Time Physiological Status Monitoring (RT-PSM) systems, BANs focused on physiological status monitoring, also have tactical applications.

Both combat and noncombat military personnel endure tough environmental conditions and physical stresses that can lead to a variety of health issues, such as hypothermia, hyperthermia, musculo-skeletal injuries, hypoxia, and dehydration. It is well documented within the armed forces that the monitoring of real-time physiological data through an RT-PSM system can aid in anticipating the onset of these conditions and could improve soldier health and readiness during training and in the field [1], [2]. For instance, members of a chemical, biological, radiological and nuclear defense (CBRND) team, who are often required to wear fully-encapsulating personal protective equipment, face significant risk of heat exhaustion which could be mitigated by providing CBRND team leaders a means of monitoring their team members' core body temperatures to properly coordinate actions [3]. In addition to improving the health and resilience of soldiers, a RT-PSM system would also be useful for increasing a team's situational awareness and providing actionable intelligence for mission planning.

The need for security in the BANs specifically (and in the largely similar Internet of Things (IoT) space) is receiving ever more attention in the media and academic communities, especially with respect to medical devices where integrity and availability of a system can be a matter of life and death. Diabetic Jay Radcliffe, for instance, demonstrated a threat to his insulin pump by compromising the wireless channel and shutting it down [4].

The consequences of targeted adversarial attacks on BANs and tactical RT-PSM systems can be severe. An adversary able to create valid messages on a BAN's wireless channel will cause data to be unreliable, impacting both the integrity and availability of the system and potentially the success of the mission. A tactical RT-PSM system would necessarily exchange sensitive health information and data relevant to mission planning in a battlefield setting. Depending on the implementation, the system components may even interconnect to long-haul radios with access to a tactical radio network. Despite its usefulness, if the proper security mechanisms are not integrated into the design, tactical RT-PSM systems could allow for more harm than good.

In this paper, we present an analysis of threats to a generalization on an existing tactical RT-PSM system architecture called OBAN. The purpose of this analysis is to help guide the development of RT-PSM systems that balance security, privacy, and utility, and we define a specific set of requirements for RT-PSM systems. While this work was performed in the context of an RT-PSM system, many of the results generalize to the broader BAN and IoT spaces where sensitive information is collected and transmitted by low-power, computationally-limited devices.

II. System Assumptions

Before we begin our threat analysis, we define our system architecture and system use case. Our goal is to choose a general use case and architecture as the basis for our analysis, to ensure our recommendations are broadly applicable to arbitrary tactical RT-PSM systems. The architecture we describe is based on a generalized version of the OBAN RT-PSM architecture described in [5]. The primary aim of the OBAN system is to improve the health, preparedness, and overall resilience of combat military personnel through real-

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. This material is based upon work supported by Defense Threat Reduction Agency under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. Air Force or Defense Threat Reduction Agency.

time monitoring of physiological data with devices capable of sustaining data collection for a period of at least 7 days.

A. Core Components

An RT-PSM implementation consists of the following core components:

- *Sensors* — Data collecting devices (e.g., electrocardiogram (ECG), core temperature, load)
- *Hub* — A radio enabled device that aggregates data from connected sensors
- *End User Device (EUD)* — A device that provides feedback to the user (in our use case this is a leader or a combat medic).

Hubs are low-power, resource-constrained devices; the OBAN prototype [5] uses boards with an ATmega 2560 microcontroller (16 MHz, 8-bit Atmel AVR architecture, 256 KB program space, 8 KB memory) [6] with a tunable narrow-band radio for sending data to the EUD. Additionally, the hubs have microSD cards to store collected sensor data for post-mission analysis. EUDs are Android-based smartphones, and thus are less resource constrained than hubs.

Team components are provisioned and configured to work together via USB connections to a configuration PC. At the beginning of a mission, multiple hubs are paired up with one or more EUDs. Each squad member is outfitted with a hub attached to sensors. The EUDs are carried by the squad leader and medics. Figure 1(a) shows an example system setup.

B. RT-PSM Use Case

For this threat analysis we consider a use case of monitoring a small team for the duration of a mission (3-7 days). Each team member has a hub device connected to several on-body sensors. The team leader and medic each have an EUD that gathers data from the hubs and displays a summary of the team's status, as shown in Figure 1(b). The system uses an application-level messaging protocol with distinct message formats intended to support the target use cases. During missions, broadcast is the fundamental communication primitive, so adversaries can take advantage of of this communication mode to eavesdrop, destroy, or replay old messages. Messages do contain a cyclic redundancy check (CRC) to protect against accidental data modification.

During a mission, the system allows for a three modes of operation:

1) Pull-style Status Updates: To monitor the physiological strain of specific team members, the squad leader would use the pull-style mode of operation. During the mission, on the squad leaders prompting or at specified intervals, the display device would request data—in this case the Physiological Strain Index (PSI)—from the nearby hubs. The hubs expose PSI as a virtual sensor that is calculated from heart rate (HR). Any hub close enough to receive the request will respond. This is the most common mode of operation.

2) Push-style Notifications: Squad leader and medic are interested in knowing if a squad member is entering a dangerous state that requires immediate action. In these cases, a hub device must push information instead of waiting for it to be collected by query from an EUD. This mode of operation would be activated, for example, if a squad member's core temperature is in a dangerously high range, such as seen with heat exhaustion or stroke. In the push-style mode of operation, a hub sends a notification addressed to a particular EUD or group of EUDs. When the message is received, the EUD acknowledges receipt provided that acknowledgement was requested in the notification. A hub will continue resending a notification periodically until the message is acknowledged or it sends the notification a set threshold number of times.

3) Streaming: The streaming mode of operation is required if a medic is providing medical attention to a soldier and would like access to the soldier's health data (e.g. ECG feed). In the stream-style mode of operation, an EUD requests that a hub send (stream) batches of a certain type of data for a specified amount of time. The hub responds with batches of data until the request has been fulfilled. Dropped batches are ignored. If the EUD wants to maintain the incoming stream it will need to send a new stream request message after the hub completes the previous stream request. This is the least common mode of operation as transmitting is power intensive [7].

III. Threat Analysis

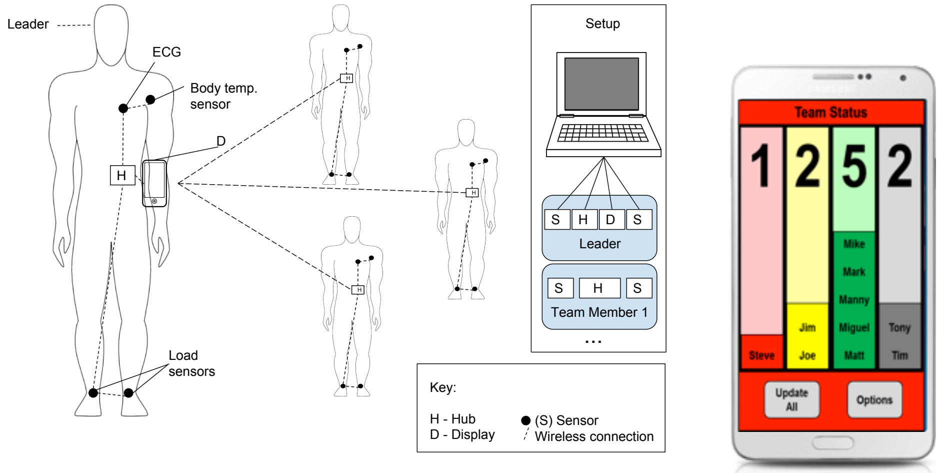
Our threat analysis considers the potential adversaries, including their capabilities and methods of attack, and the risks of such attacks, culminating in a prioritized list of threats. While this threat analysis framework should be considered qualitative, not quantitative, we endeavor to offer a comprehensive framework that can be used for a variety of adversaries, tactics, or system configurations in the RT-PSM space.

A. Adversarial Model

Following standard computer security practice, adversaries differ from one another in four main dimensions: goals, capabilities, role within the system, and attack class. Examples of specific adversaries and respective goals are given in Table I.

1) Goals: Adversaries' goals affect their motivation and choice of attacks. Consider, for instance, the difference between a squad member and a nation state. The squad member may not wish to participate in a particular mission and manipulate the system to that end (e.g. fake sensor readings). A nation state, on the other hand, might be more interested in increasing its situational awareness by determining presence of troops and acquiring the associated physiological data. A nation state adversary might thus mount an attack very different in stealth and scale from one employed by a squad member.

2) Role: Adversaries relate to the system in different ways; an adversary may be an *outsider* or an *insider*. An insider is someone who has a legitimate role in the system's operation, development, or maintenance (e.g., a user, a manufacturer, a system administrator). An outsider is an entity that comes or puts itself in contact with the system (e.g., civilians near troops



(a) Tactical RT-PSM system setup

(b) Example EUD display, showing status of squad members.

Fig. 1. OBAN RT-PSM System

TABLE I
EXAMPLE ADVERSARIES WITH ASSOCIATED GOALS AND ROUGH CAPABILITY LEVEL

	Adversary	Example Goal	Capabilities
Outsiders	Script kiddie	Create personal amusement by bragging about system disruption	Tier I
	Hacktivist	Disrupt the system or publicize sensitive information for political gain	Tiers II-III
	Nation state	Decrease the situational awareness of RT-PSM system users	Tiers V-VI
Insiders	Squad member	Malingering	Tiers I-II
	Squad leader	Improve unit appearance by faking physiological data	Tiers I-II
	System administrator	Profit from health information extracted from the system	Tiers III-IV
	Hardware/Software supplier	Profit from health information extracted from the system	Tiers IV-V

with an RT-PSM deployment, an opposing military force, etc). The level of access provided by a particular role plays a part in what attacks an adversary can successfully execute.

3) Capabilities: Mounting attacks requires a set of capabilities, which might include the ability to receive communications, ability to send communications, knowledge of the RT-PSM message protocol, etc. An adversary's capabilities are a function of their resources; to describe adversary capabilities we adopt the hierarchy presented in [8]. This report describes three main tiers of adversaries separated, in part, by resource level. Tier I and II attackers spend on the order of \$10s of dollars, Tier III and IV attackers spend on the order of \$1Ms, and Tier V and IV attackers spend on the order of \$1Bs. The higher the tier, the larger the resources and the more capabilities the attacker can obtain.

The report stipulates that Tier I and II attackers use code and exploits written by others, Tier III and IV attackers can write their own code and discover vulnerabilities, and Tier V and VI attackers are highly organized and able to implant vulnerabilities at the development level. In other words, the higher the tier the greater the level of *sophistication*. Tier I attackers, like "script kiddies" in Table I, are *unsophisticated* and Tier VI attackers, like a nation state, are highly *sophisticated*. Note, however, that level of access within the system also plays a role in this calculus. For example, a hardware manufacturer can embed vulnerabilities that would normally require Tier V level expenditures without actually spending these resources — they already have arbitrary access to the hardware platform. Similar logic applies to software manufacturers and system administrators — all these insiders are in a very trusted position with respect to the system's eventual security.

We model the following specific capabilities necessary to stage attacks against the RT-PSM system:

- *Receive RF* — The ability to receive transmissions on the appropriate frequencies.
- *Send RF* — The ability to send transmissions on the appropriate frequencies.
- *Receive Message* — Decipher an RF transmission into a message through knowledge of the application-level messaging protocol.
- *Send Message* — Construct a valid message through knowledge of the application-level messaging protocol.

- *Hub HW/SW Mod.* — Ability to modify hardware or software on the hub devices.
- *EUD HW/SW Mod.* — Ability to modify hardware or software on the EUD devices.
- *Hub Capture* — Obtain a fielded hub device.
- *EUD Capture* — Obtain a fielded EUD device.

4) Attack Class: When considering attacks, we separate them into *passive*, *network active* or *full-scope* attacks, as defined below:

- *Passive* — passive attacks can use data sent over the wireless communications channel.
- *Network active* — active attacks involve reading, creating, or destroying transmissions on any communications channel.
- *Full-scope* — full-scope attacks are not limited to the communications channel and may include software modification, hardware modification, and device capture.

Attack class is related to an adversary's resources or desire for stealth. In many environments passive attacks are generally seen as "cheaper" to mount than active attacks. In a tactical RT-PSM system, this is not necessarily true. Passive attacks require the co-location of hardware to listen for RF-transmissions, due to the fact that our system components only have a broadcast range of about 5-6 meters. The amount of hardware needed to listen to transmissions from a moving RT-PSM system deployment and the ability to access readings from the hardware that heard the transmissions could be expensive. This is one of the unique, inherent advantages of the low-power RF transmissions used by the OBAN system.

B. Threat Analysis Methodology

To analyze the risk presented by a particular threat we use a qualitative method based on a approach detailed [9]. This guide recommends using a standard model where *risk* is a function of *impact* and *likelihood*. We compute risk as the product of impact and likelihood, where impact is a subjective measure of the magnitude of harm that can be expected to result from a successful attack, and likelihood is a subjective measure of the probability that a vulnerability or set of vulnerabilities will be discovered and exploited by an attacker.

To estimate the impact to the RT-PSM system function, we define threat impact to be the maximum loss of confidentiality, data or source integrity, or availability due to the attack. To help estimate these values, we considered the extent to which an attack would result in loss of confidentiality, loss of data or source integrity, or loss of availability. We rank each of the quantities on a scale from 0 to 5—5 corresponding the largest loss possible and 0 corresponding to no loss.

To estimate threat likelihood, we consider an adversary's ability to obtain the requisite capabilities, his motivation to perform an attack and its alignment with adversary's goals, and the difficulty of finding a vulnerability and exploiting it to execute the attack.

C. Threats

In this section, we present threats to the system and rank them using the methodology described in Section III-B. Many of the security concerns that BANs face are identified in [10] and [11]; while both of these papers are not specific to tactical RT-PSM systems, they offer detailed exploration of security concerns in the context of resource-constrained, RF-enabled devices. We identify additional threats that challenge the security of our tactical RT-PSM system, including threats to the communication interface, the device software, and the device hardware. Table II describes the attacks to the system and the capabilities required by adversaries to mount the attacks[1].

Table III shows how the attacks on the system affect the standard system security properties that inform our impact metrics:

- The *confidentiality* column shows to what extent attacks are successful at exfiltrating data from the system. Majority of attacks aim to learn identifying or health-related information from the system and; consequently, most entries in this column are non-zero. Attacks that leak a larger quantity of data or more sensitive data received higher ratings.
- The non-zero entries in the *data integrity* column correspond to attacks that enable modification of data undetected by the system. Note that certain attacks that may result in message corruption, e.g. denial of service, are not in this group, since these issues are detected by checking the message's CRC code. On the other hand, attacks like individual privacy compromise (F1) and group data or source spoofing (F4) that rely on hardware/software modifications cannot be detected by the system.
- The *availability* column shows how much attacks disrupt our system's PSM service. Active attacks like (A2) privacy compromise (on demand) are shown as having an effect on availability because they cause the system components to transmit more frequently, reducing battery life; furthermore, such attacks do not respect the medium access control scheme and might interfere with legitimate message traffic.
- The last column, *source integrity*, shows what attacks require or may involve impersonation of certain entities. Existing OBAN implementation assumes that communicating entities are legitimate and non-befouled system components. The non-zero entries correspond to the attacks that take advantage of this naive assumption.

In Table IV presents our estimates for the likelihood of adversaries obtaining the capabilities necessary to mount attacks against RT-PSM system. When estimating these likelihood values, we relied on adversary descriptions and associated resource level as described in Table I. More specifically, we model the following conditions:

[1] In some cases, multiple sets of capabilities would enable an attack; we give the most common set for each.

TABLE II
RT-PSM System Threats vs. Required Capabilities

	Attack Name	Attack Description	Capabilities Required							
			Receive RF	Send RF	Receive Message	Send Message	Hub HW/SW Mod.	EUD HW/SW Mod.	Hub Capture	EUD Capture
Passive	P1. Detect presence/location (opportunistic)	Observe presence of communication on RF frequencies used by RT-PSM system	✓							
	P2. Identify team roles (opportunistic)	Observe communication patterns (e.g. query/response) to identify squad leader	✓							
	P3. Identify individuals (opportunistic)	Observe unique identifiers of devices in communication contents	✓		✓					
	P4. Privacy compromise (opportunistic)	Learn sensor data from communication contents	✓		✓					
Active	A1. Detect presence/location (on demand)	Spoof query message to trigger a response; detect/locate responding devices	✓	✓		✓				
	A2. Identify individuals (on demand)	Spoof query message to trigger a response; parse response for unique ID	✓	✓	✓	✓				
	A3. Privacy compromise (on demand)	Spoof query message to trigger a response; parse response for sensor data	✓	✓	✓	✓				
	A4. Identity spoofing	Send fake response data from a particular device	✓	✓	✓	✓				
	A5. Battery drain	Send “wake up” preamble repeatedly		✓						
	A6. Jamming	Send garbage messages to prevent others from receiving successfully		✓						
Full-Scope	F1. Individual privacy compromise (on demand)	Modify HW/SW on hub to broadcast sensor data as desired	✓		✓		✓			
	F2. Individual data spoofing	Modify HW/SW on hub to send incorrect message data in response to queries					✓			
	F3. Group privacy compromise	Modify HW/SW on EUD to leak all collected sensor data						✓		
	F4. Group data or source spoofing	Modify HW/SW on EUD to store or display incorrect data to leader/medic						✓		
	F5. Individual privacy compromise (post hoc)	Learn sensor data for an individual stored on the SD card							✓	
	F6. Group privacy compromise (post hoc)	Learn sensor data for a group stored on the SD card								✓

TABLE III
RT-PSM System Threats vs. Impact

Attack Name	Loss of...			
	Confidentiality	Data Integrity	Availability	Source Integrity
P1. Detect presence/location (opportunistic)	1	-	-	-
P2. Identify team roles (opportunistic)	2	-	-	-
P3. Identify individuals (opportunistic)	3	-	-	-
P4. Privacy compromise (opportunistic)	4	-	-	-
A1. Detect presence/location (on demand)	2	-	2	2
A2. Identify individuals (on demand)	3	-	2	2
A3. Privacy compromise (on demand)	5	-	2	2
A4. Identity spoofing	4	-	2	2
A5. Battery drain	-	-	4	-
A6. Jamming	-	-	5	-
F1. Individual privacy compromise (on demand)	3	-	2	-
F2. Individual data spoofing	-	3	2	3
F3. Group privacy compromise	5	-	1	-
F4. Group data or source spoofing	-	5	-	5
F5. Individual privacy compromise (post hoc)	3	-	-	-
F6. Group privacy compromise (post hoc)	5	-	-	-

TABLE IV
RT-PSM System Adversaries vs. Likelihood of Obtaining Capabilities

Adversary	Capabilities							
	Receive RF	Send RF	Receive Message	Send Message	Hub HW/SW Mod.	EUD HW/SW Mod.	Hub Capture	EUD Capture
Script kiddie	10%	20%	10%	20%	-	-	-	-
Hacktivist	80%	80%	80%	80%	-	-	10%	10%
Nation state	100%	100%	100%	100%	100%	100%	80%	80%
Squad member	20%	20%	20%	20%	80%	40%	40%	40%
Leader/Medic	20%	20%	20%	20%	40%	80%	60%	60%
System admin	-	-	-	-	80%	80%	80%	80%
HW/SW supplier	-	-	-	-	100%	100%	-	-

- Our model for a *script kiddie* adversary implies someone with little sophistication but with access to easily purchasable hardware and downloadable tools. Since the radio components are readily available, and software for parsing message data is not difficult to obtain, we believe this adversary can obtain capabilities to send and receive messages. However, putting the whole system together requires some effort and the motivation for this adversary is fairly low, thus the overall likelihood is rated at 20%.
- A *hacktivist* adversary is similar in nature to *script kiddie*. However, hacktivists differ in having a much stronger motive, which may embolden them (though with low probability) to attempt capturing a hub or EUD device. Because a hacktivist’s motivation is higher, the corresponding likelihood of obtaining capability to send and receive messages is rated higher as well.
- Our model for a *nation state* adversary is one that is able to obtain any of the required capabilities. Capturing hub or EUD devices may prove more difficult, so those receive less than 100% likelihood.
- A *squad member* is a legitimate user of the system, and thus has access to the hardware and software running on both hubs and EUDs. This adversary’s ability to put

together a system from readily-available components may be higher than that of a *script kiddie*, but the motivation is lower, so the ranking for sending/receiving messages (independent of the device they already have) remains at 20%. Due to more access to the system, this adversary has a higher likelihood of modifying a hub or an EUD, or possibly stealing one from another squad member or leader.

- A *leader/medic* adversary is similar to the *squad member* model; however, this adversary has greater access to EUDs, thus the corresponding change in likelihood assignments.
- Our model for a *system admin* is someone who is in charge of provisioning the system for operation and thus has ample opportunity to modify hardware or software on hubs or EUDs, as well as steal one of the devices after field deployment.
- A *hardware/software supplier* of course has ample opportunity to insert malicious trojans into the hardware or software of the device they are creating.

While the specific values presented in this table are certainly subjective, we sanity-checked that the general relationship between adversaries and the capabilities they can obtain, as well as the relative likelihood of obtaining capabilities between the adversaries corresponds to the descriptions in [8].

TABLE V
TOP RT-PSM THREATS BASED ON ESTIMATED SYSTEM RISK

Attack	**Adversary**	**Risk (0-5)**
A3. Privacy compromise (on demand)	Nation state	5
A6. Jamming	Nation state	5
F3. Group privacy compromise	Nation state HW/SW Supplier	5
F4. Group data or source spoofing	Nation state HW/SW Supplier	5
A5. Battery drain	Nation state	4
P4. Privacy compromise (opportunistic)	Nation state	4
A4. Identity spoofing	Nation state	4
F6. Group privacy compromise	Nation state System Admin	4
A3. Privacy compromise (on demand)	Hacktivists	4
A6. Jamming	Hacktivists	4
F3. Group privacy compromise	Leader/Medic System Admin	4
F4. Group data or source spoofing	Leader/Medic System Admin	4
P4. Privacy compromise	Hacktivists	3
A4. Identity spoofing	Hacktivists	3
A5. Battery drain	Hacktivists	3

Table V presents the top-ranked threats against RT-PSM given our adversary models. This ranking was obtained by computing risk as a product of attack's impact to the system (maximum value across Table III) and attack's likelihood (minimum value across required capabilities in Table IV). We selected the maximum impact to highlight where the attack is most damaging; this assumes loss of confidentiality, data integrity, availability or source integrity are equally damaging to the system. We selected the minimum likelihood for obtaining required capabilities since the likelihoods listed in the table are often not independent, and the minimum likelihood represents the "limiting reagent" notion of capability acquisition.

As expected, the more capable adversaries pose the most threat; however, it appears that hacktivist-level attacks can cause as much impact to the system (in certain categories) as nation states. Most of the top threats center on loss of confidentiality due to leakage of sensor data that represents the health information of RT-PSM users; however, the ways of achieving this privacy violation vary significantly. While loss of privacy is certainly undesirable, these threats do not by themselves make the system unusable.

Another group of top threats pertains to information integrity, enabling adversaries to spoof identity of sender or fake the data itself. Since integrity violations bring into question the trustworthiness of the system, they are potentially more worrisome than privacy risks. For example, a leader or medic can be misled about a team member's health status resulting in incorrect decisions that risk the mission and the team's well-being.

Finally, the *jamming* and *battery drain* attacks also make an appearance. These attacks strike at the availability of the RT-PSM system to perform its function; if these attacks are relatively easy to mount, this risk brings the reliability of the resulting system into question.

IV. REQUIREMENTS FOR RT-PSM SYSTEM SECURITY

Informed by the analysis in Section III-C, we would like to reduce the risk of threats resulting from cyber and EW attacks to an acceptable level of risk. In order to accomplish this, we can decrease the likelihood of a threat (e.g., increase the difficultly in obtaining the necessary capabilities to mount the attack) or reduce the impact of the threat (e.g., increase the systems ability to recover from a certain attack).

To reduce threat to the RT-PSM system, we propose the following security requirements, tailored to RT-PSM systems.

- *Data integrity* — Data in transit between a hub and an EUD should not be corrupted or modified without detection. This is required to mitigate several of the identify spoofing attacks.
- *Authentication and Authorization* — Components should be able to verify that a particular entity (or group of entities) created a message. This is required to mitigate attacks that rely on spoofing identity of a system user (e.g. squad leader), who may have privileges that other members do not (e.g. requesting status updates). This capability would help mitigate attacks A1-4, F2, and F4. Furthermore, an authorization service would allow us to revoke privileges from misbehaving devices, like those that result from F2 and F4.
- *Data confidentiality (encryption)* — Data should only be readable to properly authenticated and authorized components of our system. Parties outside our BAN should not be able to read sensor data in flight or from the memory or storage of a compromised device. The second requirement may be difficult to achieve given that we are required to store any cryptographic keys in

device memory. Encrypting the data in transit will help mitigate attacks P3, P4, A1-A3; encrypting data at rest will mitigate F5-F6.

- *Data freshness* — Authentication and confidentiality are not enough to prevent harm from active attacks that replay valid messages. In order to prevent replay attacks, hubs and EUDs must be able to ascertain the freshness of received messages by including and verifying a timestamp, sequence number, or nonce in the message.
- *Software integrity checking* — Using code signing or other methods of checking software integrity can help mitigate attacks F1-F4 by verifying that software placed on hubs and EUDs has not been tampered with to leak data or provide incorrect information to the squad leader. While hardware modifications may still be able to accomplish these attacks, they are typically much more expensive to execute successfully.
- *Availability and Sustainability (power)* — Hubs and displays should always be able to send and receive data. All components of our system should support data collection for the duration of a mission (3-7 days)[2]. Any means of achieving our other requirements must take this into account. For instance, encryption and decryption algorithms should not be overly expensive in terms of required network bandwidth or computational power.

The requirements are in no particular order, since a precise ranking would be use case dependent. For instance, availability may not be as important to an application constantly streaming ECG data as it might be for an application notifying users of exposure to hazardous chemical agents. That said, these properties are applicable to the majority of tactical RT-PSM systems. Designing and building technologies that can provide these properties in low-power devices is an ongoing research effort at MIT Lincoln Laboratory.

V. Related and Future Work

In this section, we consider the next steps necessary to create a secure tactical RT-PSM system architecture. To support system requirements detailed in Section IV, we need to identify appropriate cryptographic techniques that will work in low-power devices without compromising our system's original goal of improving the health and resilience of noncombat military personnel and first-responders. Although much of the research around BANs and wireless sensor networks has gone into making them possible and useful, an increasing number of researchers are investigating the problem of how to provide cryptographic services to resource-constrained devices.

In [12], [7], the authors construct a secure wireless sensor network built on resource-constrained devices that communicate exclusively with a more powerful central base station. The system aims to provide data confidentiality, data authentication, data integrity, and data freshness. The authors evaluate several block ciphers, and settle on running a finely tuned RC5 [13] cipher in counter mode, due to the cipher's small code size and high speed. For message authentication, they use CBC-MAC [14], allowing them to reuse the same RC5 block cipher. A lot of their design decisions are relevant to our tactical RT-PSM system, but they do not offer a complete solution for our use case due to placing strong trust assumptions in the central base station and low data rates that would not support RT-PSM streaming mode of operation.

Much of the BAN research focuses on implantable and wearable devices in the context of modern medicine [11], [15], [16], [17], [18]. In medicine, small embedded devices are responsible for relaying sensitive patient information or administering doses of medication. The need for security and privacy in this domain comes as a result of increased legislation around protecting patient information and understanding of the consequences of an insecure system; however, the hacking of medical devices is far from the number-one risk to public health [17]. Security mechanisms create additional opportunity for bugs and can slow down regulatory approval [16]; as a result, typical BAN components have been designed to transmit unencrypted data on unauthenticated channels, allowing eavesdropping and identity spoofing attacks.

In order to build a trustworthy system designers must (1) consider security early in the development process, (2) encrypt sensitive information (at rest and in transit), (3) develop a realistic threat model, and (4) use industry-standard cryptographic building blocks [18]. The last design goal proves the most difficult to apply in practice. Cryptographic building blocks are not available for the most resource-constrained devices. Medical device manufactures do not make their source code public and the research community has not produced any complete, widely-accepted solutions. While many authentication and key agreement protocols exist, majority require computational power or code space exceeding capacity of these resource-constrained devices.

Significant efforts have been expended on porting solutions from existing computing environments. For instance, researchers have gone through great lengths to tune the AES block cipher for lightweight applications. The best known hardware implementation of AES-128 fits in 2400 gate equivalents [19]—an impressive accomplishment[3] but may still be incompatible with our system components' other goals (e.g., low-cost and low-current draw during sleep) [10], [20]. This motivates the development of lightweight cryptographic primitives and BAN-specific authentication techniques.

Recently, the U.S. National Security Agency developed Simon and Speck—families of block ciphers designed for severely resource-constrained environments and optimized for hardware and software implementations, respectively. Simon and Speck require a fraction of the power that optimized AES cores do for equivalent encryption strength [20]. Similarly, the SoK literature study evaluates several BAN-specific au-

[2] Hub and EUD lifetime depends on the exact amount of time spent in each of the three modes of operation. We assume that the bulk of time is spent in *push* or *notify* modes and that the *streaming* mode is rare.

[3] To put this in context, according to [10], the amount of power it takes certain AES circuitry to encrypt a 29-byte packet is 10 times less than it takes a TI MSP430g2553 (an extremely low-power micro-controller) to turn on!

thentication techniques, including relying on biometrics, close proximity, or out-of-band channels (e.g. audio or video) for authentication purposes [11].

Lightweight cryptographic primitives and BAN-specific authentication techniques are pieces of the solution for providing security mechanisms to our RT-PSM system, but there is also a need for ultra light-weight key management and key distribution. Key management and distribution systems handle the generation, storage, exchange, and replacement of the cryptographic keys which enable the cryptographic primitives. Strong cryptographic primitives are powerless without equally solid key management[4]. Future tactical RT-PSM applications may not allow for pre-placement of keys; for these applications, light-weight, usable key management and key distribution solutions, such as the Lincoln Open Cryptographic Key Management Architecture [22], will be necessary.

One of the challenges in developing general purpose security mechanisms for BANs is that compute resources, power resources, and specific use cases differ drastically. Tactical RT-PSM system components fall somewhere between medical devices and fitness trackers. Medical devices are on the extreme end of power efficiency[5] and in the absolute worst case a compromise of the wireless channel could result in death. Fitness trackers on the other hand are typically recharged once per day and in the worst case a compromise of the wireless channel would result in a small privacy violation.

VI. Conclusion

In this paper, we have provided an adversarial model and methodology for analyzing threats to a prototype of a tactical RT-PSM system. The analysis in Section III-C shows what threats present the most risk to the system. We have given areas for future work, mainly the need to determine what mechanisms are best suited to provide the security requirements derived in Section IV. Significant work remains in comparing and demonstrating the feasibility of the different mechanisms in low-power devices used for RT-PSM. Our hope is that this analysis and the security building blocks we develop will be useful to RT-PSM systems and to broader BAN-related and IoT applications.

References

[1] I. of Medicine (US) Committee on Metabolic Monitoring for Military Field Applications, “Monitoring metabolic status: Predicting decrements in physiological and cognitive performance.” The National Academies, Tech. Rep., 2004.

[2] D. A. Brock and P. D. Horoho, “Army medicine 2020 campaign plan,” Tech. Rep., 2013. [Online]. Available: https://ameddciviliancorps.amedd.army.mil/CivilianCorps.aspx?ID=b2c81aa1-4d69-4219-a74d-90d5bcbfffbf

[3] W. Tharion, A. Potter, C. Duhamel, A. Karis, M. Buller, and R. Hoyt, “Real-time physiological monitoring while encapsulated in personal protective equipment,” *Journal of Sport and Human Performance*, vol. 1, no. 4, 2013.

[4] J. Radcliffe. (2011, aug) Hacking medical devices for fun and insulin: Breaking the human scada system.

[5] J. Biddle, D. Brigada, A. Lapadula, M. Buller, and S. Mullen, “Oban: An open architecture prototype for a tactical body sensor network,” in *Body Sensor Networks (BSN), 2013 IEEE International Conference on*, May 2013, pp. 1–6.

[6] *ATMEL 8-BIT MICROCONTROLLER WITH 4/8/16/32KBYTES IN-SYSTEM PROGRAMMABLE FLASH DATASHEET*, Atmel, 2015.

[7] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “Spins: Security protocols for sensor networks,” Secaucus, NJ, USA, pp. 521–534, Sep. 2002.

[8] *DoD, Resilient Military Systems and the Advanced Cyber Threat*. Defense Science Board Washington DC, 2013. [Online]. Available: http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

[9] R. S. Ross, *SP 800-30 Rev 1, Guide for Conducting Risk Assessments*. Gaithersburg, MD, United States: National Institute of Standards & Technology, 2012.

[10] W. Trappe, R. Howard, and R. S. Moore, “Low-energy security: Limits and opportunities in the internet of things,” *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan 2015.

[11] M. Rushanan, A. Rubin, D. Kune, and C. Swanson, “Sok: security and privacy in implantable medical devices and body area networks.” Johns Hopkins University, Computer Science, Baltimore, MD, USA, 1466, 2014. [Online]. Available: https://spqr.eecs.umich.edu/papers/rushanan-sok-oakland14.pdf

[12] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler, *Ambient Intelligence*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, ch. TinyOS: An Operating System for Sensor Networks, pp. 115–148.

[13] R. L. Rivest, *Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, ch. The RC5 encryption algorithm, pp. 86–96.

[14] M. Bellare, J. Kilian, and P. Rogaway, “The security of the cipher block chaining message authentication code,” *J. Comput. Syst. Sci.*, vol. 61, no. 3, pp. 362–399, Dec. 2000.

[15] J. Haigh and C. Landwehr, “Building code for medical device software security,” 2015. [Online]. Available: http://cybersecurity.ieee.org/images/files/images/pdf/building-code-for-medica-device-software-security.pdf

[16] W. Burleson, S. Clark, B. Ransford, and K. Fu, “Design challenges for secure implantable medical devices.” University of Massachusetts Amherst, Department of Electrical and Computer Engineering, Amherst, MA, 01003, USA, 2012. [Online]. Available: https://spqr.eecs.umich.edu/papers/49SS2-3_burleson.pdf

[17] K. Fu and J. Blum, “Controlling for cybersecurity risks of medical device software,” *Commun. ACM*, vol. 56, no. 10, pp. 35–37, Oct. 2013.

[18] W. Burleson, S. Clark, B. Ransford, and K. Fu, “Design challenges for secure implantable medical devices,” in *Design Automation Conference (DAC), 2012 49th ACM/EDAC/IEEE*, June 2012, pp. 12–17.

[19] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, “Pushing the limits: A very compact and a threshold implementation of aes,” in *Advances in Cryptology EUROCRYPT 2011*, ser. Lecture Notes in Computer Science, K. Paterson, Ed. Springer Berlin Heidelberg, 2011, vol. 6632, pp. 69–88.

[20] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, “Simon and speck: Block ciphers for the internet of things,” Cryptology ePrint Archive, Report 2015/585, 2015, http://eprint.iacr.org/2015/585.pdf.

[21] L. Constantin. (2015) Millions of embedded devices use the same hard-coded ssh and tls private keys. http://www.infoworld.com/article/3009667/security/millions-of-embedded-devices-use-the-same-hard-coded-ssh-and-tls-private-keys.html.

[22] (2012) Tech notes: Lincoln open cryptographic key management architecture. https://www.ll.mit.edu/publications/technotes/TechNote_LOCKMA.pdf.

[23] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses,” in *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, ser. SP ’08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 129–142.

[4] The lock to your front door could be top of the line, but still completely ineffective against people trying to break into your home, if you tape the key to the door. This example sounds silly, but plenty of software and hardware developers have released equivalently flawed systems [21].

[5] A pacemaker, for instance, must last on several years on a non-rechargeable battery [23].